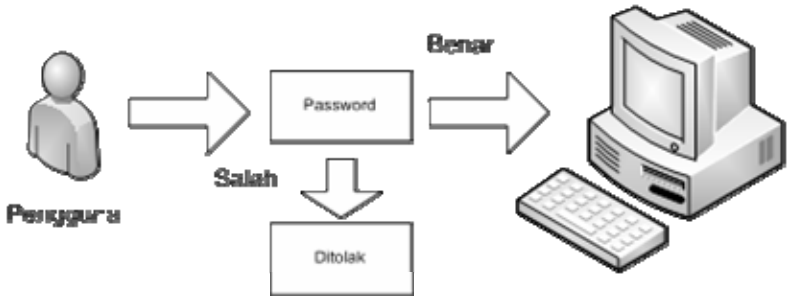
Bab 01

PassworD untuk PemuLa

Dalam bahasa Indonesia, password sering diterjemahkan dengan istilah kata sandi. Password berfungsi untuk perlindungan (proteksi) dan bersifat rahasia.

Dengan demikian, hanya orang yang tahu password saja yang bisa membuka data ataupun mengakses layanan. Orang tidak bisa sembarangan membuka data ataupun menggunakan suatu layanan karena harus tahu passwordnya. Password berisi deretan karakter yang dapat berupa huruf, angka, dan simbol.



Password telah diterapkan untuk autentikasi berbagai layanan. Dalam transaksi perbankan, kita semua mengenal adanya ATM (Anjungan Tunai Mandiri). ATM mengharuskan pemilik kartu ATM

untuk menghafal dan merahasiakan password yang biasanya hanya berupa nomor. Password tersebut sering disebut dengan Personal Identification Number (PIN).

Di internet, banyak website yang mengharuskan pengguna memasukkan *user name* (nama pengguna) dan password untuk mengakses layanan. Mulai dari email, forum, data, web hosting, situs berita, dan masih banyak lagi. Password yang berhubungan dengan komputer, biasanya dapat menggunakan seluruh karakter standar, yaitu kombinasi huruf, angka, dan simbol.

Contoh login ke layanan email Google (http://gmail.google.com)

Berkaitan dengan penggunaan komputer, password dapat digunakan untuk memproteksi data dan sistem. Data yang diproteksi bisa berupa file, sedangkan sistem yang diproteksi bisa berupa program aplikasi, sistem operasi, dan BIOS komputer.

1.1 Kelebihan dan Kelemahan

Password merupakan salah satu cara untuk melakukan autentikasi. Apakah autentikasi itu? Kata ini berasal dari bahasa Yunani yang berarti autentik. Password bertujuan agar klaim pengguna bahwa dia adalah orang yang berhak menggunakan layanan/data, dapat dikonfirmasi oleh sistem.

Ada banyak cara yang dapat digunakan untuk melakukan autentikasi. Secara garis besar dapat dibagi menjadi tiga sebagai berikut.

- Faktor pengetahuan.

  Disebut juga dengan istilah: *something what you know*. Hanya pengguna yang tahu informasi tertentu saja yang dapat mengakses data dan layanan. Informasi ini bersifat rahasia dan dapat berupa password, *pass phrase*, ataupun PIN (Personal Identification Number).

- Faktor kepemilikan.

  Disebut juga dengan istilah: *something what you have*. Hanya pengguna yang memiliki barang tertentu saja yang dapat mengakses data dan layanan. Tentu saja barang tersebut bersifat unik dan tidak bisa sembarangan ditiru oleh orang lain. Barang tersebut dapat berupa kartu identitas (*ID card*), token, HP (*Hand Phone*), dan sebagainya.

Token dengan merk dagang VeriSign

- Faktor keturunan.

  Disebut juga dengan istilah: *something what you are*. Hanya pengguna sendiri yang dapat mengakses data dan layanan. Autentikasi dilakukan dengan pengenalan ciri-ciri pengguna secara langsung. Bisa menggunakan banyak metode, mulai dari pengenalan suara, sidik jari, retina mata, pengenalan wajah, dan sebagainya.

Fingerprint (pengenalan sidik jari) pada laptop

1.1.1 Kelebihan Password untuk Autentikasi

Password tentu saja bersifat praktis. Pengguna hanya perlu menghafal kode password (*what you know*) tanpa harus menggunakan berbagai alat tambahan.

Bandingkan dengan teknologi biometrik untuk pengenalan ciri-ciri pengguna (*what you are*). Tentu saja dibutuhkan teknologi pengenalan semacam sidik jari, retina mata, telapak tangan, dan sebagainya.

1.1.2 Kelemahan Password untuk Autentikasi

Selain kelebihannya yang bersifat praktis, penggunaan password juga mempunyai kelemahan, terutama diakibatkan oleh dua faktor:

- Kecerobohan Pengguna

  Dapat terjadi jika pengguna ceroboh dalam mengatur passwordnya. Mulai dari memilih password yang gampang ditebak, password tidak dijaga dengan baik sehingga bocor, pengguna lupa passwordnya sendiri, atau password digunakan secara sembarangan.

Contoh: Setiap kali password diketikkan, maka pada saat itulah bisa terjadi insiden pencurian password. Insiden kecil seperti gerakan tangan Anda diamati orang lain saat mengetik password, dapat menyebabkan password Anda dijebol.

- Kelemahan Sistem

  Dapat terjadi jika sistem tersebut memang cukup lemah dan dapat dibobol. Artinya, yang salah bukan penggunanya tetapi memang sistem itu sendiri lemah.

  Contoh: Password BIOS komputer. Bagi pengguna yang tahu, password BIOS dapat dihilangkan (*reset*) dengan cara memindahkan *jumper* pada motherboard.

1.2 Serangan untuk Menjebol Password

Password dapat dijebol dengan berbagai teknik. Faktor yang sering dibidik untuk dieksploitasi adalah kecerobohan pengguna dan kelemahan sistem.

Sebelum membahas cara mengamankan password, kita akan membahas teknik serangan terhadap password. Dengan demikian, materi lebih jelas dan Anda tahu mengapa mengamankan password benar-benar penting.

Teknik menjebol password hanya dibahas secara umum. Untuk detailnya, akan dibahas di bab-bab berikutnya.

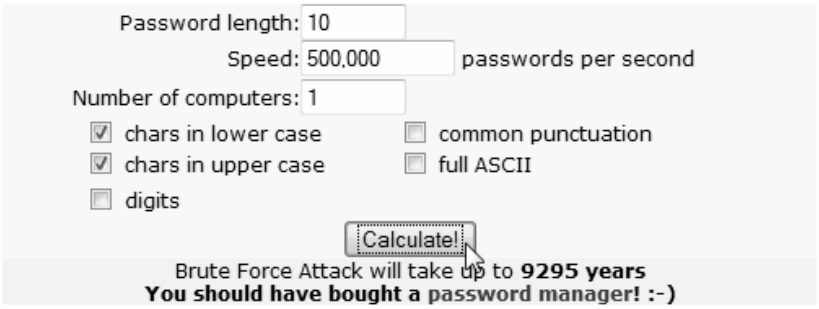
1.2.1 Brute Force Attack

Brute force merupakan teknik menjebol password dengan cara mencoba memasukkan banyak password secara berulang-ulang dan otomatis. Keberhasilan cara ini ditentukan oleh lemah kuatnya password. Jika karakter untuk menuliskan password hanya sedikit, misalnya 1-4 huruf, maka dapat dengan mudah dijebol dalam hitungan menit. Semakin panjang password, akan semakin lama prosesnya.

Untuk mengetahui berapa lama waktu yang dibutuhkan untuk menjebol password dengan *brute force*, Anda dapat menghitungnya

sendiri dengan aplikasi Brute Force Calculator. Anda dapat menghitungnya secara langsung dengan membuka alamat website **http://lastbit.com/pswcalc.asp**.

Di bawah ini contoh penghitung waktu yang dibutuhkan untuk menjebol password dengan panjang password 10 karakter, kecepatan brute force 500000 password tiap detik.



Menghitung lamanya jebol password dengan brute force attack

Pada prakteknya, lama waktu yang diperlukan untuk menjebol password dengan jumlah karakter yang sama bisa bervariasi. Di tengah jalan, bisa jadi password yang dimasukkan oleh aplikasi brute force sudah benar.

Di bawah ini tabel berisi daftar tipe file yang sering diproteksi dengan password.

Dokumen	Tipe File	Keterangan
PDF	.pdf, .eps	Portable Document Format
RAR	.rar	File terkompresi dengan format RAR
ZIP	.zip	File terkompresi dengan format ZIP
Office Word	.doc,. docx	File dokumen ketikan
Office Excel	.xls, .xlsz	File spreadsheet

Untuk menjebol password file-file dokumen dengan brute force attack, Anda dapat menggunakan berbagai jenis software. Teknik ini akan dibahas pada Bab 2.

1.2.2 Dictionary Attack

Cara yang sedikit lebih canggih untuk menjebol password adalah menggunakan *dictionary* (kamus). Teknik ini mirip dengan *brute force attack*. Jika brute force mencoba menjebol password dengan semua karakter yang mungkin, teknik ini menggunakan kamus (*dictionary*) sehingga tidak semua karakter akan dimasukkan begitu saja. Hanya kata-kata tertentu atau kombinasi karakter tertentu saja digunakan.

Teknik ini lebih mudah menjebol password jika pengguna menggunakan kata atau karakter standar. Misalnya kombinasi huruf yang mudah ditebak, kata dalam bahasa Inggris/Indonesia, nama daerah.

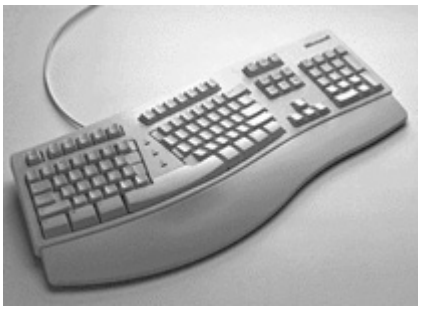
1.2.3 Keylogger

Keylogger merupakan perangkat untuk merekam kombinasi huruf/ karakter yang diketikkan oleh pengguna melalui keyboard. Keylogger dapat berupa software (perangkat lunak) maupun hardware (perangkat keras).

Dengan merekam dan menganalisis huruf yang diketikkan pengguna, Anda dapat memperkirakan password yang digunakan oleh pengguna tersebut.

Keylogger dalam bentuk hardware sulit dideteksi. Berbeda dengan software keylogger yang masih mungkin dikenali dengan aplikasi yang mampu melihat proses (*process)* pada komputer.

Perangkat keras dapat berupa keyboard itu sendiri yang juga berfungsi sebagai keylogger. Tentu saja keyboard jenis ini tidak beredar luas di pasaran.



Keyboard dilengkapi dengan keylogger.
Terlihat seperti keyboard biasa

Ada juga hardware tambahan yang dapat dipasangkan ke dalam komputer dan akan merekam ketikan yang Anda buat.

Contoh USB flash disk yang juga berfungsi sebagai keylogger

http://www.keelog.com/

1.2.4 Social Engineering

Social engineering merupakan teknik pendekatan untuk memanipulasi orang lain sehingga mau memberikan password. Teknik ini lebih berkaitan dengan hubungan sosial, dan tidak harus menggunakan teknik hacking.

Social engineering dapat dilakukan dengan cara menipu melalui email, website, telephone, maupun komunikasi langsung. Sebagai

contoh, Anda dapat mengintip password yang sedang diketikkan seseorang dengan berpura-pura menemaninya berinternet.

Sedangkan social engineering melalui email, website, dan telephone dapat dilakukan dengan penipuan. Intinya, Anda berpura-pura menjadi seseorang yang punya otoritas, misalnya Administrator, lalu meminta user memberitahukan passwordnya.

1.2.5 Phising

Phising berasal dari kata fishing, yang berarti memancing. Phising dilakukan dengan cara memancing pengguna sehingga pengguna tertipu dan mau mengetikkan passwordnya. Cara yang sering dilakukan adalah phising dengan email dan website.

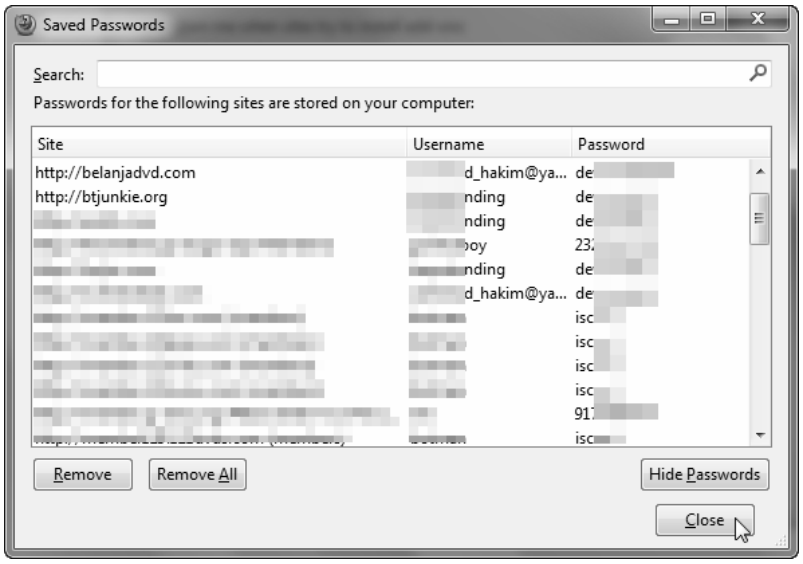
Phising melalui email dilakukan dengan mengirimkan email kepada calon korban. Di dalam isi email sudah dimasukkan link (*tautan*) yang digunakan untuk menipu korban.

Misalnya tersedia link ke **mail.yahoo.com**. Padahal link tersebut tidak mengarah ke Yahoo; tetapi ke website lain dengan tampilan mirip dengan situs Yahoo Mail. Setelah pengguna tertipu dan mengetikkan password, maka password tersebut telah direkam dan dapat dipakai oleh pihak lain.

1.2.6 Eksploitas Kelemahan Sistem

Masih banyak pengguna yang tidak paham dengan sistem yang mereka pakai. Akibatnya, pengguna tipe ini sangat rawan terhadap serangan keamanan.

Contoh: Banyak orang masih belum tahu bahwa Firefox dapat menyimpan password. Jika tidak waspada, password dapat ikut tersimpan sehingga dapat dibuka oleh orang lain.



1.2.7 Sniffing

Sniffing merupakan teknik untuk mengamati aliran data yang lewat melalui jaringan. Dengan kata lain, sniffing juga dapat digunakan untuk menyadap data rahasia termasuk password.

1.3 Mengamankan Password

Ada banyak faktor yang harus diperhatikan untuk memastikan password Anda tetap aman. Mulai dari pemilihan password, menggunakan password, dan mengetahui sistem dengan baik agar terhindar dari pencurian password.

1.3.1 Memilih Password

Pengamanan pertama harus dimulai dari memilih password yang akan dipakai. Password yang buruk akan mudah ditebak oleh orang lain. Selain itu, password yang lemah juga mudah dijebol dengan teknik *brute force* dan *dictionary attack*.

Pertanyaannya adalah: Bagaimana memilih password yang baik? Ada dua hal yang harus dipertimbangkan:

- Password susah ditebak orang lain maupun oleh aplikasi *brute force/dictionary attack*. Jika password Anda gampang ditebak, bisa jadi akan dibobol orang dengan mudah.
- Password mudah diingat. Bagaimana jika password Anda sangat sulit ditebak tetapi juga sulit dihafal? Tentu saja bisa berbahaya kalau Anda sendiri lupa passwordnya. Karena itu, password harus sulit ditebak tetapi gampang diingat.

Untuk membuat password sulit ditebak ada beberapa trik yang dapat Anda terapkan, yaitu:

- Jangan menggunakan kata umum dalam bahasa Indonesia maupun bahasa Inggris. Juga jangan menggunakan kata umum seperti nama orang, nama daerah, ataupun tanggal lahir.

  Kata yang terlalu umum akan mudah ditebak oleh orang lain serta lebih rentan dijebol dengan *brute force attack* yang memanfaatkan kamus (*dictionary*).
- Jangan menggunakan jumlah karakter yang sedikit. Karakter yang sedikit sangat rentan dijebol dengan aplikasi brute force attack. Dianjurkan menggunakan password minimal 8 karakter.
- Sebaiknya menggunakan kombinasi angka dan huruf besar/kecil. Jangan hanya menggunakan huruf kecil saja.

Untuk membuat password yang mudah diingat tentu susah-susah gampang. Intinya harus seunik mungkin tetapi mudah Anda ingat.

Trik yang Penulis lakukan adalah menggunakan gabungan beberapa suku kata dari daftar kata yang penting. Untuk kata, Anda dapat menggunakan nama, alamat, tempat lahir, dan nama lain yang penting bagi Anda. Untuk angka, dapat menggunakan tanggal lahir, tanggal hari raya, nomor pegawai/mahasiswa, nomor telepon, dan nomor lain yang Anda ingat.

Contoh password: 192madRachKayuloko

Password di atas dapat dijelaskan sebagai berikut.

- **192**. Nomor awal IP yang banyak digunakan untuk membangun jaringan (IP private network biasanya 192.168.0.0). Kebetulan Penulis benar-benar ingat dengan nomor ini.
- **madRach**. Diambil dari nama Rachmad Hakim S.
- **Kayuloko**. Nama desa di mana Penulis dibesarkan.

Anda dapat berimprovisasi sendiri sehingga menghasilkan password yang sulit ditebak, sulit dijebol, tetapi dapat Anda ingat dengan mudah.

1.3.2 Menggunakan Password

Setiap kali mengetikkan password untuk menggunakan layanan, maka harus dilakukan dengan hati-hati. Itulah saat kritis di mana password dapat dicuri. Tentu Anda tidak mau ada kamera pengawas yang mengintip gerakan tangan Anda saat mengetik password.

Untuk itu, pastikan Anda menggunakan komputer yang aman. Pengguna rental komputer dan warung internet juga harus berhati-hati agar tidak salah pilih.

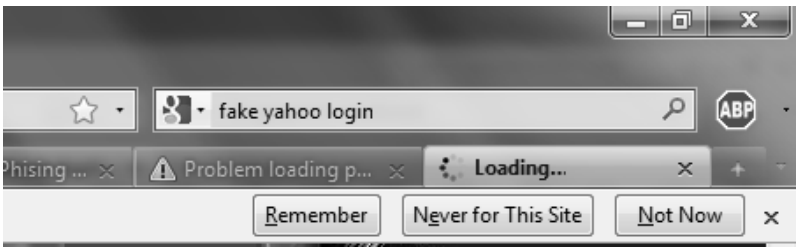
1.3.3 Memahami Sistem dengan Baik

Dengan memahami cara kerja sistem, Anda akan tahu titik-titik lemah pada sistem tersebut. Dengan demikian, Anda dapat lebih berhati-hati dalam menggunakan layanan.

Sebagai contoh, banyak pengguna baru internet yang tidak mengetahui bahwa *internet messaging* seperti Yahoo Messenger dapat menyimpan password. Bahkan ada yang tidak melakukan log out setelah menggunakan layanan seperti Yahoo email.

Setiap kali melakukan login untuk mengakses data dan layanan, maka selalu lakukan log out. Selain itu, jangan pernah menyimpan password ke dalam komputer yang digunakan untuk publik.

Opsi Remember my ID & password digunakan untuk menyimpan password



Opsi menyimpan password setelah melakukan login

1.4 Software Password Manager

Password harus dijaga agar tetap rahasia dan aman dari orang lain. Di sisi lain, Anda tidak boleh lupa dengan password. Dua hal yang berlawanan tersebut dapat menjadi kesulitan tersendiri. Untuk itulah hadir program aplikasi yang dapat dipakai untuk mengatur password.

Aplikasi	Website	Keterangan
KeePass Password Safe	http://keepass.info	Gratis, open source, OSI certified
My Password Manager	www.mypasswordmanager.com	Gratis
PassPack	www.passpack.com	Gratis, berbasis web

Pada bab ini, Penulis akan membahas dua buah software yang dapat digunakan untuk manajemen password: Password Assistant dan Password Generator.

Aplikasi password manager yang dibahas dalam buku hanyalah sebagai contoh. Anda dapat meneliti kembali dan memastikan bahwa program tersebut benar-benar aman dan password tidak dicuri oleh program yang Anda gunakan.

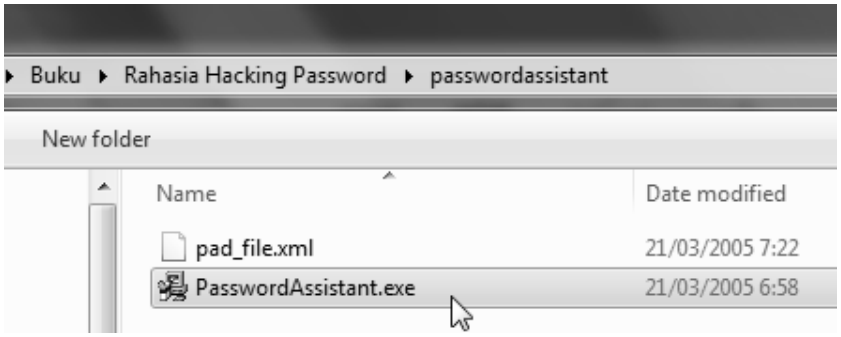
1.4.1 Password Assistant

Aplikasi Password Assistant dapat Anda unduh (*download*) pada salah satu alamat website di bawah ini:

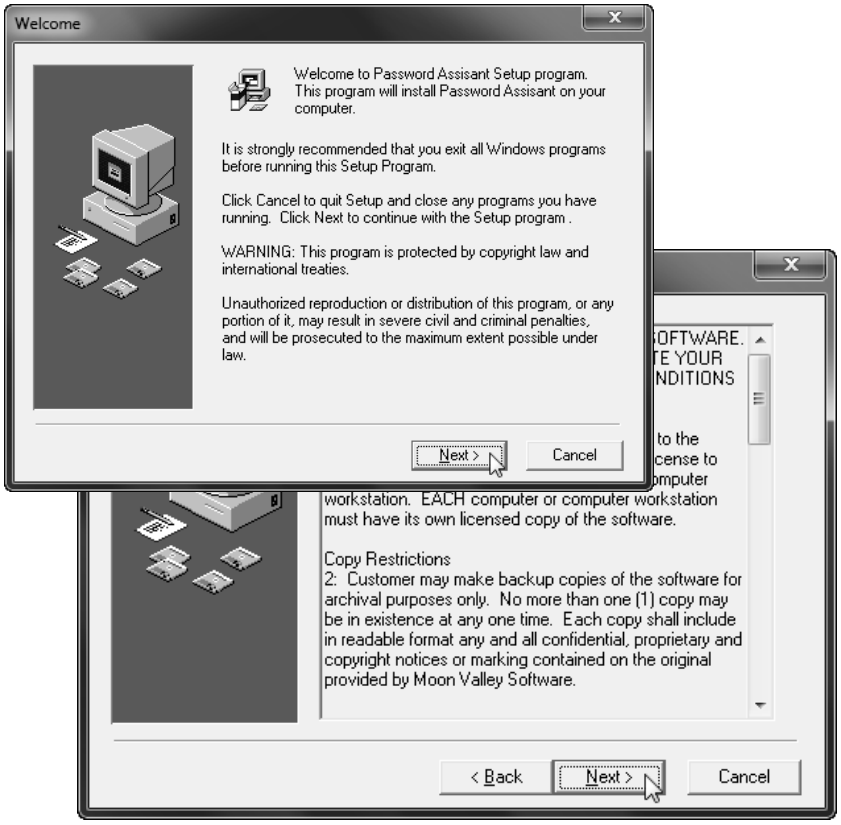
- **http://password-assistant.smartcode.com/info.html**
- **http://www.moonvalley.com/**

Setelah proses download selesai, lakukan instalasi dengan langkah-langkah sebagai berikut:

1. Jalankan instalasi dengan klik ganda pada file hasil download, yaitu **PasswordAssistant.exe**.



2. Klik **Next** untuk melanjutkan instalasi.
3. Klik **Next** untuk menyetujui perjanjian.

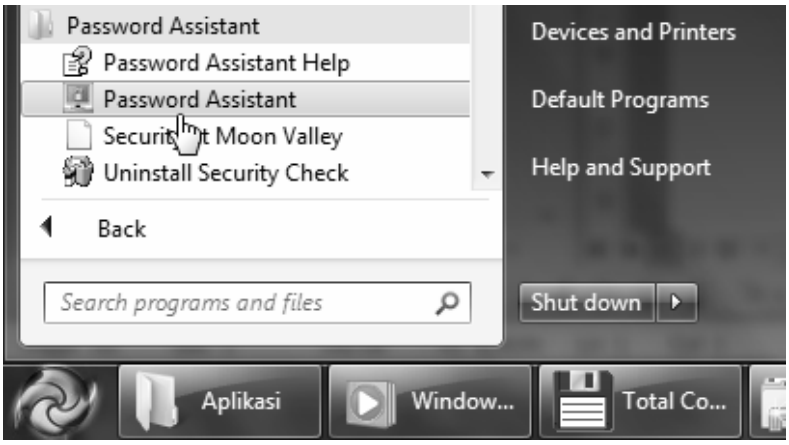


4. Klik **Next** untuk menggunakan folder default untuk menyimpan file-file instalasi.
5. Klik **Next** untuk memulai instalasi.

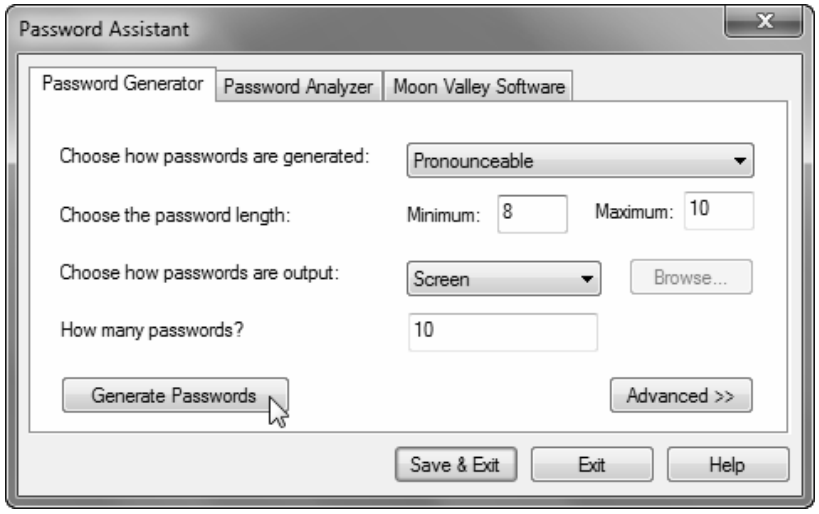
6. Klik tombol **Finish** untuk menyelesaikan instalasi.

Setelah program Password Assistant selesai diinstal, Anda dapat mulai menggunakannya dengan cara berikut.

1. Klik tombol **Start Windows** lalu pilih menu **All Programs** > **Password Assistant** > **Password Assistant**.



2. Anda dapat menggunakan aplikasi untuk membuat password. Caranya, tentukan konfigurasi yang akan digunakan untuk password lalu klik tombol **Generate Passwords**.



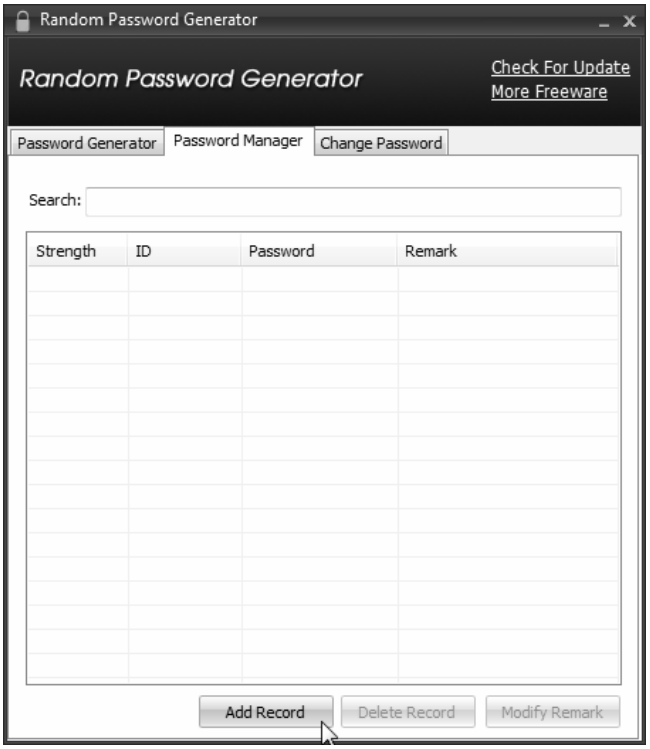
3. Maka akan muncul daftar password yang dapat Anda gunakan. Klik **OK** untuk menutup kotak dialog.

4. Sedangkan untuk menganalisis kekuatan password, klik tab **Password Analyzer**.
5. Ketikkan password yang akan dianalisis. Pada contoh ini, Penulis mengetikkan **192madRachKayuloko**. Klik tombol **Analyze Now**.
6. Maka akan muncul informasi di bagian bawah.

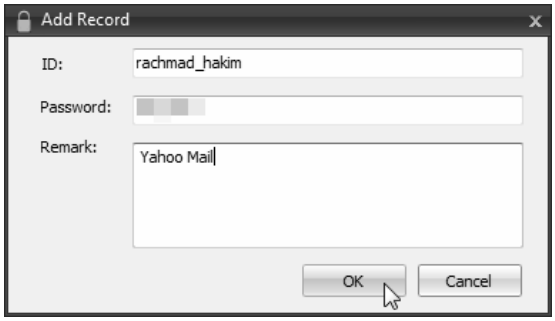
1.4.2 Password Generator

Password Generator bisa digunakan untuk membuat (*generate*) dan menyimpan password. Aplikasi ini dapat diunduh dari situs **http://www.iobit.com/password-generator.html** atau instal langsung dari DVD buku pada file **\Aplikasi\ PasswordGeneratorSetup.exe**.

1. Setelah instalasi selesai, jalankan program Password Generator.
2. Klik tab **Password Manager**. Simpan password dengan klik tombol **Add Record**.



3. Ketikkan ID dan password yang akan disimpan lalu klik tombol **OK**.



4. Maka daftar password akan disimpan.